VÍNCULOS
ENERO - JUNIO DE 2010
VOLUMEN 7 ■ NÚMERO 1

Sistema multiagente para la detección de operaciones de consulta, envío y borrado de correos no autorizados

Multiagent system for the detection of query operations, delivery and email deleting unauthorized

Juan Carlos Guevara B.
Luis Felipe Wanumen S.
Gloria Andrea Cavanzo N.
César Valdés L.

Fecha de recepción: abril 30 de 2010
Fecha de aceptación: mayo 28 de 2010

Resumen

En este artículo se describe un sistema multiagente capaz de detectar operaciones de consulta, envío y borrado de correos en un sistema de correo electrónico. El trabajo implicó el montaje y configuración del sistema de correo electrónico *Exchange*, la creación de un sistema multiagente —siguiendo la metodología AOPOA con agentes en los clientes y el servidor, de tal forma que permitieran detectar las operaciones de consulta—, envío y borrado de correos no autorizados, la definición de un protocolo de prueba del sistema y el análisis de los resultados, obtenidos de la aplicación del sistema multiagente. Adicionalmente, se creó un *firewall* que permitiera registrar las mismas operaciones de detección y comprobar el funcionamiento del sistema multiagente.

Palabras clave: sistema multiagente, sistema de correo electrónico, seguridad informática, amenazas de seguridad, ataques.

Abstract

We describe a multi-agent system which detects query, send and delete operations in an e-mail system. This includes installation and configuration of the Exchange mail system, a multi-agent system with AOPOA methodology, which detects clients and agent's server query operations, sending and deleting illegal emails, defining a test protocol system and analysis of the results of applying multi-agent system. Additionally, a firewall that could record the same operations for detecting and monitoring the performance of multi-agent system was created.

Key words: multi-agent system, e-mail system, internet security, security hazards, internet attacks.

Introducción

La seguridad informática es una fuente de preocupaciones, que aumentan cada día, debido a que gran parte de la información que manejamos está controlada por sistemas informáticos (correo electrónico, cuentas bancarias, ventas, facturación, presupuestos, etc.), a través de los cuales continuamente fluyen los datos e información personal. Una de las principales fuentes de ataque son los sistemas de comunicación electrónicos y sobre todo en Internet; y muchos usuarios no on conscientes de este riesgo (Rodríguez).

El correo electrónico es una de las herramientas de comunicación más utilizadas en Internet, una de las aplicaciones que más ataques reciben y es sobre la que urge trabajar para el perfeccionamiento de su seguridad (Stephen T.K.; 1993 y Schenier; 1998). Este problema ha sido afrontado a través de esquemas de seguridad, entre los cuales cabe mencionar los que brindan criptografía — (Pretty Good Privacy PGP (Zimmermann; 1995), Privacy Enhanced Mail - PEM (Linn; 1993), SMIME (Ramsdel; 1999) — y los que establecen protocolos de correo electrónico certificado que protegen tanto al emisor como al receptor, entre otros (Stallinfs; 2002). Sin embargo, estos esquemas no cubren todos los aspectos de seguridad en los sistemas de correo electrónico (Hsie-Hau; 2002). La estructura de Internet está basada en el protocolo de comunicaciones IP en el que la información del transmisor tiene que ser leída por un número indeterminado de *routers* y dispositivos antes de llegar al receptor. Esta secuencia hace vulnerable el acceso y la seguridad de la información, así como a la red por donde se transmite (Martin y de Quinto; 2003). Algunos de los componentes que se deben tener en cuenta para comprender las vulnerabilidades y las soluciones necesarias de seguridad de transmisión y recepción de un mensaje de correo electrónico son: el software de correo electrónico del cliente, la cuenta de correo electrónico del emisor (cliente), el mensaje (que puede ser consultado, enviado o borrado de manera no autorizada), el servidor de correo electrónico del proveedor de servicios (servidor), el canal de comunicación, los protocolos de envío (SMTP) y recepción (POP3) de mensajes y las decisiones de entrega de información por parte del cliente.

En la actualidad existen virus y gusanos que han sido diseñados para infectar millones de computadores en el mundo a través de Internet, utilizando como medio de propagación los sistemas de correo electrónico. El coste estimado de las consecuencias que generaron los virus y gusanos en el año 2005 fue de 19.000 millones de dólares. Además, las empresas están afectadas por correo electrónico no solicitado (conocido como *spam*). Se estima que el correo no deseado alcanza un rango entre el 50% a 70% de todo el correo electrónico transmitido por Internet y son el medio de transporte de aplicaciones que intentan acceder a la información de las empresas. Por ello, los sistemas de correo electrónico son un punto crítico para las empresas ya que los servidores de correo electrónico son repositorios de datos clave para las operaciones diarias de las empresas, a los cuales personas malintencionadas (piratas informáticos y emisores de *spam*) pueden acceder a través de la red corporativa. Es por ello que el correo electrónico se ha convertido en el medio más utilizado para ocasionar infecciones de virus y a través de él sucede el 88% de los incidentes corporativos reportados en el 2004 (Microsoft).

Dado el rápido desarrollo y la gran utilidad de las aplicaciones y servicios basados en Internet, éstos son cada día más importantes para la vida de las personas y las organizaciones. Muchos usuarios y organizaciones utilizan servicios *online* (como Google Docs, Dropbox, gestores de contenidos, etc.), en vez de software de oficina. Los servicios sociales en línea (como Facebook, Linkedin) permiten participar en actividades sociales, información en línea (por ejemplo, Twiter), en ofertas de productos empresariales y ventas *online* (Deremate.com, Amazon.com). Es evidente que con estas utilidades los riesgos de seguridad y privacidad se incrementan, ya que, para el uso de estos servicios y aplicaciones en línea, los usuarios deben crear cuentas, para las cuales usan su cuenta de correo electrónico, y al proporcionar esta información permiten ataques a la cuenta y a los sistemas de correo electrónico empresarial (Lei, et al.; 2010).

Como parte de las medidas contingentes, las organizaciones requieren investigar y desarrollar tecnologías que permitan detectar el ataque de personas malintencionadas a los sistemas de correo electrónico y proteger la información almacenada (Microsoft). En ese sentido, los sistemas multiagente ofrecen una alternativa de solución atractiva y eficiente, frente a esta clase de problemas, ya que conforman sociedades de agentes que tienen fines comunes y cumplen tareas complejas mediante coordinación y colaboración (Eurologic).

Frente a estas expectativas y en este contexto, el proyecto desarrollado se planteó las siguientes preguntas: ¿Cómo desarrollar un sistema multiagente que permita detectar operaciones de consulta, envío y borrado de correos electrónicos no autorizados? ¿Qué elementos se deben tener en cuenta en la configuración de un esquema de seguridad de un sistema de correo electrónico? ¿Cómo montar un esquema de detección de operaciones de consulta, envío y borrado de correos electrónicos apoyado en un sistema multiagente?

Marco conceptual

Seguridad Informática

Concepto

Una forma de definir la seguridad es la ausencia de riesgo o la confianza en algo o alguien, lo cual depende del contexto donde se esté. La seguridad informática debe proteger la confidencialidad, la integridad y disponibilidad de la información (Rodríguez; Eurologic), las cuales se definen como:

Confidencialidad: la información sólo puede ser conocida por individuos autorizados.

Existen varias técnicas para lograr confidencialidad, una de ellas es el cifrado. Dentro de los ataques para romper la privacidad de la información, está interceptar la información que se envía por la red o la intrusión directa en los sistemas donde se almacena la información (Rodríguez; Eurologic; Álvarez).

Integridad: se refiere a la seguridad para que la información sólo sea modificada por entidades autorizadas durante la transmisión. La modificación incluye cualquier operación posible sobre la misma como borrado, copia, escritura, creación, etc. También es necesario mantener la integridad de la secuencia de datos para asegurar que la información no se repita o se pierda y que la secuencia de bloques de datos recibidos no haya sido alterada (Eurologic) (Álvarez).

Disponibilidad: e la información se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite por las entidades autorizadas. Esto implica evitar la negación de servicio (Eurologic; Álvarez).

Amenazas

Una amenaza se puede definir como una acción o un acontecimiento en el entorno que pueda atentar contra la seguridad (confidencialidad, integridad, disponibilidad); también, como la violación potencial de la seguridad de un sistema (Rodríguez; Álvarez). Los sistemas informáticos están expuestos a tres tipos básicos de amenazas (Rodríguez):

Intencionadas: de usuarios no autorizados, tanto internos como externos, al sistema, quienes se pueden clasificar según sus intenciones: curiosos y maliciosos. Los usuarios curiosos intentarán acceder a los sistemas por simple curiosidad y los maliciosos intentan acceder a los sistemas con intenciones dañinas, dentro de esta clasificación se encuentra el robo de equipos (Rodríguez).

No intencionadas: se producen normalmente a partir de usuarios inexpertos que, por ignorancia, negligencia o descuido, pueden borrar información, crear agujeros de seguridad al no actualizar los programas debidamente o facilitar sus contraseñas personales (Rodríguez).

Programas maliciosos: son programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema, como virus informáticos, gusanos informáticos, troyanos, bombas lógicas o programas espías (Rodríguez).

Naturales o de fuerza mayor: en las que no actúan las personas pues son eventos naturales como incendios accidentales tormentas e inundaciones, terremotos, incendios, inundaciones o fallo en los equipos (cortocircuitos, cortes del sistema eléctrico, otros) (Rodríguez).

Ataques

Se pueden clasificar por los efectos que causan en los sistemas:

Interrupción: Un recurso del sistema es destruido o se vuelve no disponible. Es un ataque contra la disponibilidad a los equipos ya sea por destrucción del hardware o software (Álvarez).

Intercepción: una entidad no autorizada consigue acceso a un recurso. Es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora. Un ejemplo es la utilización de troyanos para la obtención de datos de forma ilícita (Álvarez; Navartiva).

Modificación: una entidad no autorizada no sólo consigue acceder a un recurso, también es capaz de manipularlo. Es un ataque contra la integridad. Los troyanos y virus realizan este tipo de ataques (Álvarez; Navartiva).

Fabricación: una entidad no autorizada inserta objetos falsificados en el sistema. Es un ataque contra la autenticidad. La inserción de mensajes falsos en una red o la adicción de datos a un archivo son ejemplos de este tipo de ataques (Rodrígez; Álvarez).

Otra posible clasificación de estos ataques es:

Ataques pasivos: obtención de información sin alterar la comunicación ni los datos. Para ello se escuchan o monitorizan las comunicaciones, con el fin de obtener y analizar la información que está siendo transmitida, controlando del volumen de tráfico o controlando las horas habituales de intercambio de datos. Estos ataques son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos, pero existen formas sencillas de evitarlos como con la encriptación (Álvarez; Navartiva).

Ataques activos: que realizan modificaciones de los datos o crean datos falsos y comprenden suplantación de identidad, reactuación o captación y repetición de varios mensajes, modificación de mensajes o degradación del servicio (Álvarez; Navartiva).

Sistemas Multiagente

Concepto

Desde el comienzo de la inteligencia artificial se definió el concepto de agente, el cual es un objeto que puede percibir el entorno a través de sensores y modificar su ambiente por medio de actuadores. Cuando los agentes optimizan su ejecución se les denomina agentes racionales (Vlassis; 2007). Sin embargo, en muchas ocasiones los agentes no son entes solitarios, interactúan en forma grupal; a este grupo de agentes se les llama sistema multiagente (Vlassis; 2007).

Los aspectos fundamentales que caracterizan los sistemas multiagente son: el diseño de los agentes, el que debe hacer tanto en software como en hardware, y su comportamiento, que puede ser homogéneo o heterogéneo. El ambiente donde se desenvuelven los agentes varía según la situación, el ambiente puede ser estático o dinámico o cambiar de un estado al otro. La percepción de los agentes se hace de manera individual por cada agente, por lo tanto, la percepción del sistema multiagente es distribuida. Los agentes toman individualmente decisiones; esto significa que el sistema tiene un control descentralizado. El conocimiento en un sistema multiagente depende del conocimiento de cada agente y, por último, la comunicación es un proceso de dos vías tanto para enviar como para recibir mensajes (Vlassis; 2007).

Aplicaciones en sistemas de seguridad

Los sistemas multiagente, junto con otras técnicas de inteligencia artificial (como la visión artificial —aplicadas en biometría y reconocimiento de textos manuscritos—, redes bayesianas —problemas de spam y detección de ataques—, redes neuronales —sistemas de detección de intrusos—, sistemas inmunes artificiales —sistemas de detección de intrusos—, sistemas expertos —auditoría— y algoritmos genéticos —sistemas de detección de intrusos—), se han utilizado para el desarrollo de herramientas que apoyen la seguridad informática. Entre las aplicaciones de los sistemas

multiagente están sistemas de seguridad en redes, arquitectura segura, auditoría, sistema de verificación de integridad de archivos (Martín y de Quinto; 2003).

Los agentes han sido utilizados tanto para vulnerar las redes como para protegerlas; de hecho, la vulnerabilidad de un SMA es una de las causas de no ser utilizados en muchas aplicaciones que podrían sacar un buen beneficio de ellas. Basado en una jerarquía de dominio de dos niveles, se desarrolló (Iqbal, et al.; 2007) un SMA robusto basado en agentes Java móviles denominado "PeAgent", con un mecanismo de agente de grano fino para control de privilegios y otro de protección multinivel, que organizan el gran número de nodos de Internet en el sistema de agentes en unidades manejables. El sistema logró un entorno informático seguro para aplicaciones ampliamente distribuidas en una red de plataformas heterogéneas que facilita el desarrollo de aplicaciones seguras basadas en web. Para cubrir la necesidad de una comunicación segura entre agentes de un MAS se ha propuesto (Oliviera, et al.; 2006) un modelo de comunicación segura basadas en la sintaxis de los mensajes XML (mensajes RDF o "resource description framework") que proporciona mecanismos de seguridad (autenticación, confidencialidad, no repudio e integridad) adaptados a especificaciones de seguridad XML.

Net-Mass es un sistema multiagente distribuido que actúa como una herramienta de protección para redes con diferentes sistemas operativos y vulnerables a diversos ataques. Está integrado por agentes con características específicas de detección de intrusos y protección de sistemas primordiales de la red, los cuales utilizan diferentes técnicas de inteligencia artificial como sistemas expertos, algoritmos evolutivos y redes neuronales; cuentan con una estructura constituida de tres componentes: componente de ejecución, componente funcional y componente de comunicación, y con seis tipos de agentes: agentes de escucha, de detección de intrusos de red, de detección de virus, coordinación, de reporte y de alarma y auditoría Martín y de Quinto; 2003).

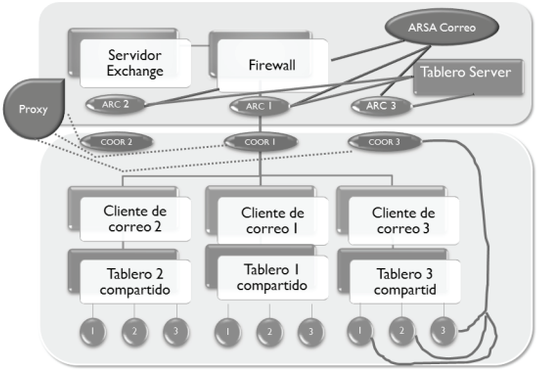
El simulador, basado en agentes para ataques contra redes de computadores ASACN, fue desarrollado para simular ataques distribuidos mediante una secuencia coordinada de actividades coordinadas por malhechores. Cada malhechor es mapeado como un agente inteligente; mientras se realiza la ejecución de un ataque distribuido, los malhechores interactúan para coordinar sus actividades (Gorodetski y Koteniko; 2002).

El Sistema Multiagente para la detección de intrusos MIDS toma decisiones basado en un procesamiento de datos, de entrada multinivel, que usa un esquema de metaclasificación; cuenta con una arquitectura conformada por un agente *demon*, que es responsable del pre procesamiento del tráfico de entrada, el cual monitorea el tráfico y extrae secuencias de eventos que son semánticamente significativas para la detección de eventos, los cuales son ordenados, almacenados en una base de datos y enviados para una posterior por otros agentes; agentes *demons*, para la identificación, autenticación y control de acceso, son quienes ejecutan operaciones de registro de resultados dentro de la base de datos y envían mensajes al agente de detección de intrusos; los agentes *demos* AD-P1 y AD-P2 son responsables de la extracción de patrones significativos de eventos y toman decisiones de acuerdo al comportamiento del usuario (Gorodetski y Kotenko; 2002).

Descripción de la solución

El proyecto consistió en el desarrollo de un sistema multiagente que permite detectar operaciones de consulta, al igual que el envío y borrado de correos en un sistema de correo electrónico. El proyecto implicó el montaje y configuración del sistema de correo electrónico Exchange, la creación de un sistema multiagente conformado por agentes en los clientes (círculos 1,2 y 3 de la figura 1) y agentes en el servidor (Arc1, Arc2, Arc3, Coor1, Coor2 y Coor3), siguiendo la metodología AOPOA (Gorodetski y Kotenko; 2002) (González y Bustacura; 2007), que permitan detectar las operaciones de consulta, envío y borrado de correos no autorizados, montaje de la plataforma de sistemas multiagente Besa, la definición de un protocolo de prueba del sistema y el análisis de los resultados obtenidos de la aplicación del sistema multiagente. Además se creó un *firewall* que permite detectar las mismas operaciones de detección y comprobar el funcionamiento del sistema multiagente. En la figura 1 se muestran los diferentes componentes del sistema.

Figura 1. Estructura del Sistema Multiagente



En el desarrollo del proyecto, primero se realizó la instalación del servidor de correo Exchange, el contenedor de agentes Besa y el *firewall*, luego se aplicó la metodología AOPOA que nos permitió obtener el sistema multiagente. Las etapas aplicadas de la metodología son las siguientes:

Identificación de casos de uso y objetivos

Para cada uno de los anteriores casos de uso se hizo una descripción. Los resultados en resumen se muestran en la siguiente tabla:

Tabla 1: casos de uso

Caso de uso: detectar operaciones de consulta de correo electrónico sospechosas	Caso de uso: detectar operaciones de envío de correo electrónico sospechosas	Caso de uso: detectar operaciones de borrado de correo electrónico sospechosas
Se realiza con agentes en el lado del servidor y en el lado del cliente, quienes tienen la habilidad para hacer consultas sospechosas de usuarios autenticados como “no”.	Se realiza con agentes en el lado del servidor y en el lado del cliente, quienes tienen la habilidad para consultas sospechosas de usuarios autenticados como “no”.	Se realiza con agentes en el lado del servidor y en el lado del cliente, quienes tienen la habilidad para consultas sospechosas de usuarios autenticados como “no”.
Requerimiento No Funcional compartido. El sistema debe funcionar con servidores de correo Exchange y en redes bajo un mismo dominio Windows	Requerimiento No Funcional compartido. El sistema debe funcionar con servidores de correo Exchange y en redes bajo un mismo dominio Windows	Requerimiento No Funcional compartido. El sistema debe funcionar con servidores de correo Exchange y en redes bajo un mismo dominio Windows

Tabla 2: objetivos

Id. Objetivo	Objetivo	Id. Objetivo padre
O1	Detectar ataques al servidor de correo	
O1.1	Detectar ataques usando técnicas de borrado masivo de correo	O1
O1.2	Detectar ataques usando técnicas de visualización masiva de correo	O1
O1.3	Detectar ataques usando técnicas de envío masivo de correo	O1
O1.1.1	Detectar ataques borrando con usuarios sospechosos	O1.1
O1.1.2	Detectar ataques haciendo borrados masivos con cuenta autorizada	O1.1
O1.2.1	Detectar ataques visualizando correos con usuarios sospechosos	O1.1.2
O1.2.2	Detectar ataques visualizando correos masivos con cuenta autorizada	O1.1.1
O1.3.1	Detectar ataques ingresando correos con usuarios sospechosos	O1.1.2
O1.3.2	Detectar ataques ingresando correos masivos con cuenta autorizada	O1.2.1

En AOPOA se hace necesaria la identificación de objetivos y hacer que esta identificación vaya concretando los detalles de los mismos con un enfoque Top-Down. Al identificar correctamente los objetivos se pueden relacionar con recursos, habilidades y entidades externas. A continuación, se muestran los objetivos identificados siguiendo AOPOA.

Identificación de tareas, e interacciones

Se obtuvo una lista de seis tareas, en donde todas tenían recursos involucrados compartidos con otras tareas. En la siguiente tabla se muestra la relación entre las tareas con las habilidades, recursos y objetivos.

Tabla 3: tareas

Nombre de la tarea	Id. del objetivo	Clase de objetivo	Recursos involucrados	Habilidades necesarias
T1	O1.1.1	OBJ-TIPO 3	R1 R3	HABILIDAD 2 HABILIDAD 5 HABILIDAD 7
T2	O1.1.2	OBJ-TIPO 3	R1 R3	HABILIDAD 2 HABILIDAD 5 HABILIDAD 7
T3	O1.2.1	OBJ-TIPO 2	R1 R4	HABILIDAD 3 HABILIDAD 6 HABILIDAD 8
T4	O1.2.2	OBJ-TIPO 2	R1 R4	HABILIDAD 3 HABILIDAD 6 HABILIDAD 8
T5	O1.3.1	OBJ-TIPO1	R1 R2	HABILIDAD 1 HABILIDAD 4 HABILIDAD 9
T6	O1.3.2	OBJ-TIPO1	R1 R2	HABILIDAD 1 HABILIDAD 4 HABILIDAD 9

Las habilidades identificadas en la última columna de la tabla anterior son las siguientes:

1. Habilidad para verificar hace cuánto tiempo se hizo la última acción de envío tipo *send*.
2. Habilidad para verificar hace cuánto tiempo se hizo la última acción de envío tipo *drop*.
3. Habilidad para verificar hace cuánto tiempo se hizo la última acción de envío tipo *view*.
4. Habilidad para recibir información del detector de solicitudes de envío de *emails*.
5. Habilidad para recibir información del detector de solicitudes de borrado de *emails*.
6. Habilidad para recibir información del detector de solicitudes de visualización de *emails*.
7. Habilidad para verificar si cambio la cláusula FROM con respecto a la solicitud de BORRADO hecha anteriormente y calcular el tiempo en el que se había hecho la anterior solicitud de este tipo.}
8. Habilidad para verificar si cambió la cláusula FROM con respecto a la solicitud de VISUALIZACIÓN hecha anteriormente y calcular el tiempo en el que se había hecho la anterior solicitud de este tipo.
9. Habilidad para verificar si cambió la cláusula FROM con respecto a la solicitud de ENVÍO hecha anteriormente y calcular el tiempo en el que se había hecho la anterior solicitud de este tipo.

Las tareas anteriores se agrupan en grupos de tal forma que se tenga una relación de que tareas pueden ser realizadas por determinados roles. De otra parte, y siguiendo el concepto de descomposición de roles, se concluye que los siguientes son los roles definitivos del sistema:

Tabla 4: roles

Rol	Rol Padre	Descripción	Tareas asignadas
SMA		Rol para la detección de ataques por parte de usuarios que intentan acceder a cuentas de un servidor de correo Exchange y realizar ataques de envío, borrado o visualización por medio de una cuenta autorizada o no autorizada en un servidor de correo	T1 T2 T3 T4 T5 T6
Rol 1	SMA	Rol para la detección de ataques por parte de usuarios que intentan usar técnicas de borrado masivo de correo	T1 T2
Rol 1.1	Rol 1	Rol para la detección de ataques por parte de usuarios que intentan hacer borrados masivos con cuenta autorizada	T1
Rol 1.2	Rol 1	Rol para la detección de ataques para usuarios que intentan hacer borrados de *emails* con usuarios sospechosos	T2
Rol 2	SMA	Rol para la detección de ataques para usuarios que usan técnicas de visualización de correos	T3 T4
Rol 2.1	Rol 2	Rol para la detección de ataques para usuarios que intentan visualizar correos con usuarios sospechosos	T3
Rol 2.2	Rol 2	Rol para la detección de ataques con usuarios que intentan visualizar correos masivos con cuenta autorizada	T4
Rol 3	SMA	Rol para la detección de ataques usando técnicas de envío de correos	T5 T6
Rol 3.1	Rol 3	Rol para la detección de ataques para usuarios que ingresan correos con usuarios sospechosos	T5
Rol 3.2	Rol 3	Rol para la detectar de ataques por usuarios que ingresan correos masivos con cuenta autorizada	T6

Tabla 5: tareas

Vinculo	Roles	Recursos en conflict	Objetivos sinérgicos	Tipo de situación	Técnica	Protocolo
Vin. 1	Rol 3.1 Rol 3.2	R2	O1.3	Objetivo común	Colaboración por asignación directa	Request Iteration Protocol
Vin. 1	Rol 2.1 Rol 2.2	R4	O1.2	Objetivo común	Colaboración por asignación directa	Request Iteration Protocol
Vin. 2	Rol 2.1 Rol 2.2	R3		Objetivo común	Colaboración por asignación directa	Request Iteration Protocol
Vin. 3	Rol 1.1 Rol 1.2		O1.1 O1.1	Objetivo común	Colaboración por asignación directa	Request Iteration Protocol
Vin. 4	Rol 2.1 Rol 2.2		O1.2	Objetivo común	Colaboración por asignación directa	Request Iteration Protocol
Vin. 5	Rol 1.2 Rol 2.1		O1.2	Objetivo común	Colaboración por asignación directa	Request Iteration Protocol

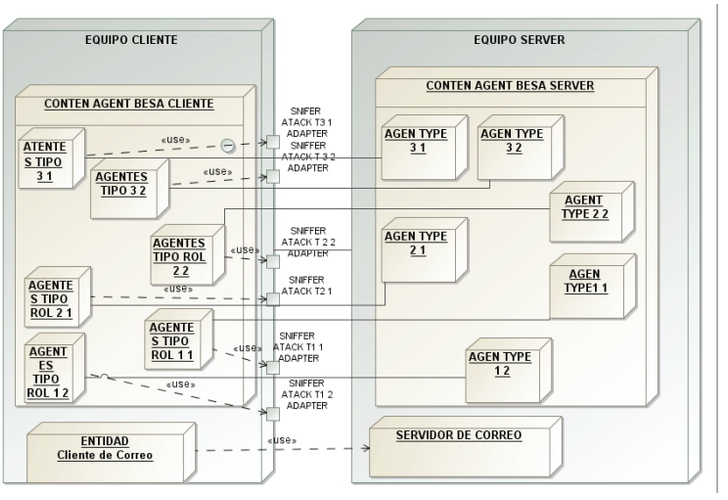
Caracterización de agentes

Con todo el trabajo elaborado hasta el momento, se pueden identificar y caracterizar los roles de los distintos agentes del sistema. A continuación se muestra la tabla definitiva obtenida como fruto de la identificación de meta agentes.

Tabla 6: Caracterización de los agentes

Meta agentes	**Roles**
Meta agente para la detección de ataques por parte de usuarios que intentan hacer borrados masivos con cuenta autorizada	Rol 1.1
Rol para la detección de ataques para usuarios que intentan hacer borrados de *emails* con usuarios sospechosos	Rol 1.2
Rol para la detección de ataques para usuarios que intentan visualizar correos con usuarios sospechosos	Rol 2.1
Rol para la detección de ataques con usuarios que intentan visualizar correos masivos con cuenta autorizada	Rol 2.2
Rol para la detección de ataques para usuarios que ingresan correos con usuarios sospechosos	Rol 3.1
Rol para la detectar de ataques por usuarios que ingresan correos masivos con cuenta autorizada	Rol 3.2

Figura 2. Arquitectura del Sistema Multiagente

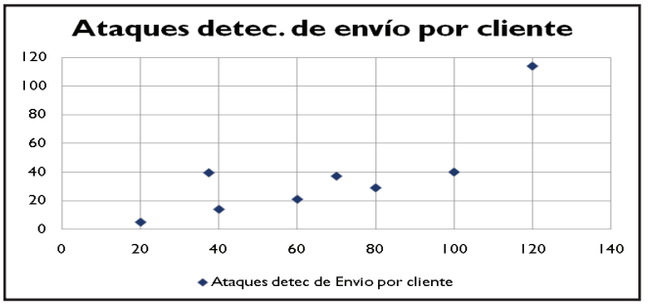


Pruebas y resultados

El sistema multiagente inicialmente se colocó en un escenario de prueba, el cual contó con la aplicación de correo electrónico Exchange en un servidor y 20 cuentas de correo electrónico. Los usuarios de las cuentas siguieron un protocolo de pruebas, donde realizaron diferentes ataques de consulta, envío y borrado de mensajes no autorizados. Los resultados obtenidos de la ejecución del sistema se muestran en las figuras X, Y y Z.

Figura 3. Ataques de envío de mensajes no autorizados

Número peticiones de envío	Ataques detec. de envío por cliente
20	5
40	14
60	21
80	29
100	40
120	114

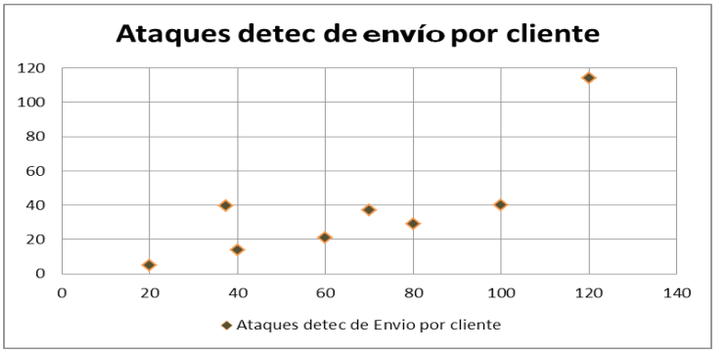


El sistema multiagente muestra que, cuando el número de ataques es 20, tan solo el 25% de ellos son detectados. Lo anterior, en tanto que, cuando los ataques son mayores, como por ejemplo en el último caso que se hicieron 120 ataques, el número de ataques detectados fue 114. La razón es que ambas pruebas se hicieron en el mismo intervalo de tiempo y los agentes están programados para que entre menos tiempo exista entre una solicitud al servidor de correo y exista otra solicitud para una misma máquina, se tendrá más tendencia a evaluarlo como un ataque sospechoso.

Estos resultados pueden ser analizados desde diversas ópticas. Una de ellas tiene que ver con el análisis concerniente a predecir el comportamiento que tiene el SMA cuando el número de peticiones de envío de ataques son grandes, con respecto al número de

peticiones detectadas. En otras palabras, se hicieron ataques al sistema y cuando el número de ataques fue 20, se detectaron 5, teniendo en cuenta que el número de ataques es para la misma cantidad de tiempo. En realidad se hicieron en 5 minutos 20 ataques y tan solo 5 fueron detectados. Pero cuando se hicieron 120 ataques el SMA detectó 114 de ellos, lo que quiere decir que, cuando los envíos son rápidos y consecutivos unos de otros, el SMA detecta mejor dichos ataques. Este comportamiento se presenta por varias razones; una de ellas es porque los agentes tienen mayor cuidado cuando se envía un evento de creación de correo que procede a otro envío en un tiempo muy pequeño. La siguiente gráfica muestra la relación entre ataques detectados vs ataques hechos:

Figura 4. Ataques detectados de envío por cliente



La interpretación que se puede dar de estos datos es que conforme crecen los ataques el SMA también aumenta, y en la misma proporción el número de ataques detectados. Esto indica que el SMA es una buena opción por su escalabilidad, la cual se presenta en la detección de ataques, no solo cuando se tienen pocos ataques sino cuando se tienen varios. Este tipo de cosas ayuda a vislumbrar que el comportamiento es lineal.

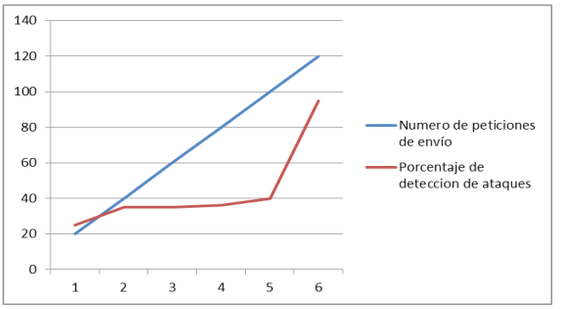
Otra forma de analizar los datos anteriores es mirar la proporción en la que se detectan ataques, en proporción con la cantidad de éstos; en otras palabras, la tabla anterior se puede escribir de la siguiente manera:

Tabla 7: Porcentaje detección de ataques

Número de peticiones de envío	Ataques detectados de envió por cliente	Porcentaje de detección de ataques
20	5	25
40	14	35
60	21	35
80	29	36,25
100	40	40
120	114	95

Y se podría hacer un gráfico comparativo entre la primera columna y la tercera:

Figura 5. Análisis de peticiones de envío y detección de ataques



El **Eje X** es el número del experimento (se numeran consecutivamente). El **Eje Y** es el número de ataques. La gráfica muestra una tendencia interesante en la que se puede vislumbrar que, a medida que el número de peticiones de ataques aumenta, también aumenta el porcentaje de detección de ataques, lo cual indicaría que si los ataque son pocos no es bueno usar un SMA; por ejemplo, si el número de ataques es 60, casi el 50 de ellos son detectados, en tanto que, si el número de ataque aumenta, se tiene que la proporción de ataques detectados, con respecto al número de ataques hechos, aumenta; esto indicaría que si tenemos muchos ataques sería más aconsejable tener un SMA.

Conclusiones y perspectivas

Los gusanos, los virus y el *spam* no son las únicas amenazas en los sistemas de correo electrónicos. El correo electrónico es un objetivo clave para los piratas informáticos, quienes lanzan ataques o colocan trampas en los sistemas de correo electrónico a fin de desconectarlos u obtener información confidencial contenido en ellos.

En el mundo interconectado de hoy, donde los usuarios requieren acceso remoto a los sistemas de correo electrónico, para así compartir información con colaboradores, con los clientes, y con los socios, es esencial asegurar el acceso a los recursos del sistema de correo electrónico.

El desarrollo de aplicaciones basadas en sistemas multiagente, para apoyar la seguridad de sistemas de correo electrónico, implica contar con agentes ubicados en el servidor y con clientes que permitan monitorear las operaciones que se realizan sobre el sistema. También el definir una estructura que permita asignar roles y tareas que deje a los agentes cumplir una misión específica.

El desarrollo del proyecto permitió conocer un área de aplicación de los sistemas multiagente y esperamos continuar desarrollando nuevas aplicaciones que permitan apoyar la seguridad de los sistemas de correo electrónico y de seguridad informática.

Referencias

Rodríguez, J. http://eciencia.urjc.es/dspace/bitstream/10115/905/1/PFC%20NIETO%20RODRIGUEZ.pdf

Stephen T.K. (1993). *Internet Privacy Enhanced Mail*. En: "Communications of the ACM". Vol. 36. No. 8. Pp. 48-60.

Schneier, B. (1995). E*Mail Security: How for Keep Your Electronic Messages Private*. New York: John Wiley & Sons, Inc.

Zimmermann, P.(1995). *The Official PGP User's Guide*. Massachusetts: MIT Press.

Linn, J. (1993). *Privacy Enhancement for Internet Electronic Mail, Part I: Message Encryption and Authentication Procedures*. *RFC 1421*, Disponible en: http://tools.ietf.org/html/rfc1421 California: IETF.

Ramsdell, B. (1999) *WMIME Version 3 Message Specification. RFC 2633.* Disponible en: http://www.ietf.org/rfc/rfc2633.txt. California: IETF.

Stallings, W. (2002). *Cryprogruphy and Nefwork Security: Principles and Prucfice*. 3rd edition. Prentice-Hall, Inc.

Hsien-Hau. C, et al. (2003). *Design and Implementation of Smartcard-based Secure E-Mail Communication. In Security Technology*, Proceedings. IEEE 37th Annual 2003 International.

Martín. A, de Quinto. F. (2003). *Manual de seguridad en internet. Soluciones técnicas y jurídicas*. Fundación Galicia.

Microsoft. . *Seguridad en el correo electrónico y colaboración de su empresa*. Disponible en: http://www.microsoft.com/spain/exchange/securemessaging/seguridad.mspx.

Lei, J., Takabi, H., Joshi, J.B.D. (2010). *Security and Privacy Risks of Using E-mail Address as an Identity. In Social Computing (SocialCom)*. IEEE Second International Conference.

Eurologic. *Conceptos básicos de seguridad informática*. Disponible en: http://www.eurologic.es/conceptos/conbasics.htm

Álvarez, M., Criptología y seguridad. Páginas de Gonzalo Álvarez Marañón. Disponible en: http://www.iec.csic.es/criptonomicon/seguridad

Seguridad de la Información (Segu-Info). Seguridad Física. http://www.segu-info.com.ar/fisica/seguridadfisica.htm

Navactiva. Clasificación y tipos de ataques contra sistemas de información. Disponible en: http://www.navactiva.com/es/documentacion/clasificacion-y-tipos-de-ataques-contra-sistemas-de-informacion_16477

Vlassis, N. (2007). *A Concise Introduction to Multiagent Systems and Distributed Artificial Intelligence*. Morgan & Claypool Publisher.Gorodetski, V., Kotenko, I. (2002). *The Multi-agent Systems for Computer Network Security Assurance: Frameworks and* Case Studies. En: "Artificial Intelligence Systems" ICAIS, IEEE International.

González, E. y Bustacara, C. (2007). *Desarrollo de aplicaciones basadas en sistemas multiagente*. Bogotá: Editorial Pontificia Universidad Javeriana. Rodríguez. J., Torres. M., González. E. (2007). *La metodología AOPOA*. En: "Revista Avances en Sistemas e Informática", Vol.4 No. 2, Septiembre.. Disponible en: http://pisis.unalmed.edu.co/avances/archivos/ediciones/Edicion%20Avances%20 2007%202/08.pdf, pp. 71-78.

Iqbal, Z., Mehmood, A., Ghafoor, A., et al. (2007) *Authenticated service interaction protocol for Multi-Agent System International Symposium on High Capacity Optical Networks and Enabling Technologies*.

Oliveira, E., Abdelouahab, Z., Lopes, D.,(2006). *Security on MASs with XML Security Specifications*. 17th International Workshop on Database and Expert Systems Applications, 2006.